GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 709
TO BE ANSWERED ON: 25.07.2025

VULNERABILITY AUDITS OF CRITICAL INFRASTRUCTURE

709. SHRI K.R. SURESH REDDY:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the details of the vulnerability audits of critical infrastructure sectors such as power, transport or banking conducted by Government during FY 2024-2025;
(b) the steps being taken to strengthen coordination between the Indian Computer Emergency Response Team (CERT-In) and State-level agencies for faster response to cyberattacks;
(c) whether Government is working to develop indigenous cybersecurity tools and reduce reliance on foreign solutions, if so, the details thereof, if not, the reasons therefor; and
(d) whether there are plans to set up sector-specific cyber emergency units or training centres to improve resilience, if so, the timeline and details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): Government remains conscious of the cyber threats to India's digital and physical infrastructure. The policies of Government of India are aimed at ensuring a safe, trusted, and accountable cyberspace for all users. Multiple initiatives have been undertaken to secure critical infrastructure sectors such as power, transport or banking for their uninterrupted and safe functioning.

CERT-IN and NCIIPC carry out cybersecurity audits under Information Technology Act and Rules made thereunder.

The details of security and vulnerability audits of critical infrastructure sectors carried out in 2024-25 are under:

Sector	CERT-In Security Audits (FY 2024-25)	NCIIPC audits (FY 2024-25)
Power & Energy	1,579	46
Transport	582	3
Banking, financial services, and insurance (BFSI	7,547	41

Total	9,708	90

CERT-IN has empaneled 200 cybersecurity organizations for carrying out these audits.

The Government has undertaken several measures to improve cyber resilience which, inter alia, includes:

1. CERT-In issues the necessary guidelines for setting up of State/sectoral Computer Security Incident Response Teams (CSIRTs).

    a. Sector-specific CSIRTs, such as CSIRT in Finance sector (CSIRT-Fin) and CSIRT in Power sector (CSIRT-Power), are operational to coordinate cyber security issues and improve cyber resilience within respective sectors.

2. Centre for Development of Advanced Computing (C-DAC) has developed a range of indigenous cyber security tools in mobile security, forensics, log collection & analytics etc. to reduce reliance on foreign solutions.

3. CERT-In has formulated a Cyber Crisis Management Plan (CCMP) for all government bodies to counter cyber-attacks and cyber-terrorism. CCMP provides strategic framework to coordinate recovery from cyber-crisis and enhance resilience.

    a. In addition, guideline documents and templates have been published to assist development and implementation of state-level/sectoral Crisis Management Plans.

4. CERT-In also regularly conducts workshops for government bodies and key organizations to sensitize them about the cyber security threat landscape and enabling them to prepare & implement the CCMP. So far, 205 such CCMP workshops have been conducted.

******